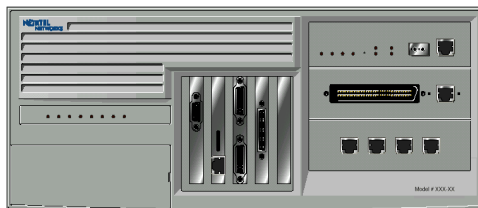


Release Notes for Nortel Networks Business Communications Manager 2.5



August 13, 2001

Version: 1.02

Date Issued: August 13, 2001

Document Status: Issued

Author: Al Campbell

Dept: Global Customer Care Services/NPI, 2108

Table of Contents

I.	Introduction	3
II.	Technical Support	3
	a. How To Get Help	3
	b. Contact Information.....	3
	c. Technical Support Access Requirements.....	4
III.	Release Notes for Business Communications Manager	
	a. New Features	5
	b. Key Issues.....	7
	c. Known Issues.....	7
	i. Platform Services.....	7
	ii. Management Tools.....	8
	iii. Core Telephony.....	10
	iv. IP Telephony.....	11
	v. Voice Applications.....	14
	vi. Data Components.....	18

I. Introduction

Business Communications Manager 2.5 is an Advanced IP communications solution for single or multi-site customers. The product unifies technologies from the voice and data world into a single platform. Business Communications Manager 2.5 is a solution that represents the convergence of telephony, computer communications, call center functions and extensive voice and data networking in the IP Telephony Network Design and support space.

II. Technical Support

a. How to Get Help

Each authorized Distributor needs a PIN code for this service, which can be obtained from the contacts below. ITAS/CTAS opens a “Heat Ticket” or “CSR (Customer Service Request)” and works a solution for the distributor.

If a problem is identified with the product, an SR (Service Request) is opened with the Technology Group for resolution.

Emergency support service is available after business hours (24x7)
The same contact numbers are utilized to access a messaging service that in turn pages an ITAS Engineer.

b. Contact information

Technical Support North America

ITAS Canada 1-800-661-4827

ITAS USA 1-800-321-2649

naitas@nortelnetworks.com

<http://www.nortelnetworks.com/itas/>

Presales Support 1-800-4NORTEL (1-800-466-7835)

Option 3 is Sales or Pre-Sales support

Access to the ITAS website can be obtained by ordering part # wwwitas or sending an email to the general mailbox at naitas@nortelnetworks.com .
After logging on to the ITAS website, you can:

- Review product documentation
- Obtain certification information
- View technical tips
- Download service packs, feature packs, or patches
- Request technical support

Technical Support EMEA

CTAS EMEA +44 (0) 1628 432400
Tel: 33 4 9296 1341
Fax: 33 49296 1598
emeahelp@nortelnetworks.com

Technical Support CALA
CTAS CALA 1-954-858-7777
csrmgmt@nortelnetworks.com

Technical Support APAC
CTAS APAC Tel +61 388664627
Fax +61 388664644
asia_support@nortelnetworks.com

c. Technical Support Access Requirements

General

All callers are required to have a Personal Identification Number to access BCM Technical Service Center (TSC)

Training

New Partners (w/o BCM or Norstar experience)-Callers must demonstrate technical competence by successfully completing complete BCM 2.5 curriculum
Existing Partners (w/Norstar experience)-Callers must demonstrate technical competence by successfully completing modified BCM 2.5 training curriculum
Existing Partners (w/ BCM experience)-Callers must demonstrate technical competence by successfully completing BCM 2.0 certification exam and BCM 2.5 Centra (delta) courses

Successful Completion=Passage of the assessment test

Additional Conditions

Existing Partners are entitled to a 90-day grace period from date of notification to achieve new product authorization requirements

New Partners callers must complete authorization requirements prior to registering for TSC access

Existing Non-Authorized callers billed at currently published per-incident rates after grace period

Calls regarding product defects or issues are non-billable

III. Release Notes

a. Business Communications Manager 2.5 New Features

Nortel Networks has implemented the following new features/enhancements in Business Communications Manager 2.5:

Platform Enhancements

- PEC III support
- New Media Bay Modules
 - CTM-8
 - 4x16 Combo
 - DECT
- NTP Client
- System Status monitor (new light board which controls fans/temperature)

Management Enhancements

- New revised management home Page
- 5 new Wizards.
 - Quick Start, Add user, Edit Template, Change DN's, DECT.
- New web based Client Install Page.
- Integrated Call Pilot Web administration.
- Web Maintenance and Support tools.
- Web based On-line documentation.
- Telephony administration enhancements.
- BRU administration via Unified Manager
- Usability enhancements (right click and tabs)

Core Telephony

- Message Waiting Indicator for Business Series Terminals
- System Wide Call Appearance (SWCA)
- Distinctive line ringing (DLR)
- MCDN over PRI enhancements
 - o Message Waiting Indicator
 - o Network Call Redirection
 - o Trunk Route Optimization
 - o Trunk Anti-Tromboning
 - o Camp on
 - o Break in
- DECT wireless support of 32 handsets and 8 base stations using integrated DECT media bay
- ISDN Supplementary features (Interoperability, Malicious Call Trace, Advice of Charge)
- System localization & ISDN support for 14 markets

- Text prompts on sets
- Application prompts on sets
- Loss Plan and tone plans
- Audio prompts for applications

IP Telephony

- Support for IP Clients (i2004 Internet Telephone & i2050 Software phone)
- Media Path Management (or redirection)
- QoS for IP stations
- Increase in simultaneous VoIP sessions Up to approx. 30 IP trunks
- Gatekeeper Interworking - Radvision

Voice Applications

Voice Mail

- Voice mail management has moved to web based Call Pilot Manager
- CCR Tree home transfer node
- Choice of Call Pilot User interface or Norstar
- Call Pilot Unified Messaging Client Support

Call Center & Call Center Reporting

- Call Center (ACD) capacity enhancements. (80 Skillsets & 250 configured agents)
- Call Routing and Overflow enhancements
- Caller Input Rules routing
- Delegated Supervisor Administration
- Auto Logout and Auto answer for agents
- CLID/DNIS Routing
- Multimedia call center support for web based caller access.
- Automatic configuration for call center reporting
- Support for IP wallboards

Other Voice Application Enhancements

- LAN CTE support for network TAPI without NT domain
- LAN CTE support for 3rd party developers
- Desktop Assistant Pro application for button labeling and programming
- Call Detail recording support for ISDN supplementary features.

Data Components (NAT, Firewall Filters, DHCP, etc...)

- PPTP Support.
- IPsec/VPN support.
- COPs client and Policy Server support.
- Multiple IP addresses/NIC.
- NAT

b. Business Communications Manager 2.5 Key Known Issues

The following issues are considered the most “serious” known issues in BCM 2.5. All of these issues are listed again in section c below and are only shown here in a brief summarized format. For more info on a specific issue please click on the issue below.

Item	Page
• Upgrade Process not currently available.	7
• DECT configuration wizard failure.	9
• Seven conference call issue.	10
• FAX over IP is not currently supported.	11
• BCM 2.0X to 2.5 IP trunk interoperability issues.	13
• ITG Interoperability considerations.	13
• Voice Mail Storage Time Issue	14
• LAN CTE server component stopping issue.	17
• QoS, IPSec, PPTP and NAT support issues.	22
• NAT currently doesn't support IP clients.	27
• WAN Card Issues with Frame Relay and PPP.	27

c. Business Communications Manager 2.5 Known Issues

The list below shows known issues with Business Communications Manager Release 2.5. Service Request (SR) numbers have been shown to help with tracking the issues. SR's are used internally at Nortel Networks to track issues.

Platform Services

Upgrade Process

- The upgrade process from BCM 2.03 to 2.5 is not currently available. The upgrade process will be available on August 31, 2001 .

NTP (Network Time Protocol)

- There is an issue with the "Maximum Time Adjustment" field of the NTP client. If this field is set to anything other than zero - e.g. 180 seconds (3 minutes) - the RFC states that if the time clock of the BCM is off by more than 180 seconds, then the time will only be adjusted by 180 seconds. This feature has been incorrectly implemented such that if the time clock is out by more than 180 seconds, there will be no time adjustment. This will be corrected in an up-issue, and at present it is recommended to keep this field set to its default value of 0.
- When NTP settings are changed they will not be picked up until the VoiceTimeSync service is stopped and restarted.

System Status Monitor (SSM)

- The SSM will not have full functionality with BCM 2.0 hardware. In order to get all of the new functionality the BCM 2.5 HW is required.

Hardware

- The expansion chassis supports only 4 ASM modules
- BCM 2.5 is only supported on BCM 2.0 H/W. Older 1.X systems cannot be used, because the MSC card will not upload new F/W properly.

Management Tools

Unified Manager

- If you are trying to open two sessions from the same BCM on the same client, the second UM will replace the first UM in the same window, to workaround this do the following: If you add the Web page mgmt.html to the end of the URL (e.g. <http://10.10.10.1:6800/mgmt.html>), a new browser window is opened taking you straight to the login window for UM. For the preinstalled client (which requires you to install the Java classes on your PC) use the URL <http://10.10.10.1:6800/preinstalled-mgmt.html>.
- Also note that setting an HTTP Proxy on a client browser will affect your ability to access Unified Manager. This is because Unified Manager uses DCOM for the communication with BCM, which is not HTTP. To get around this problem, you still can use the proxy server to access any other web pages, but not Unified Manager. To workaround this configure your web browser to have an exception for the BCM's IP address in the proxy configuration.
- When logging into Unified Manager, sometime the user may see an error message: "[Connection Failed] Failed to connect to BCM server". There are two main causes for this error message. One is that the BCM has just been rebooted and is not up yet. The other is due to a timer time-out of Microsoft DCOM while logging into Unified Manager; it happens whenever the target BCM has a large number of dial-up interfaces and/or a large number of tunnels, PPTP or IPSec, configured. Some other configuration data also contribute to this time-out as well. For this time-out case, the user can rectify the problem by applying a patch. The patch is already on the system, and the instructions are given in the following.
 1. Close all the browser windows on the client
 2. Telnet in to BCM
 3. Select Command Prompt option
 4. Go to folder C:\Program Files\Nortel Networks\Unified Manager\Patch
 5. Run "fixlogon i" to install the patch
 6. Log back into Unified Manager. If it prompts, "[Connection Failed] DCOM Server is not ready, Please try later." please click on Login button again.
- Note that doing client installs from the web interface requires a lot more free HD space on your client PC, than when doing the install through the shared "norteldt" folder. If free space on your local HD is limited, you should not

install clients from the web interface. Listed below are the HD space requirement of some Client installs from the Web.

I2050:

All languages (default)	55MB
One language only	30 MB
Personal Call Manager :	32 MB
Attendant Console Client:	64 MB
Desktop Assistant:	6 MB
Desktop Assistant Pro:	12 MB
VB Agent Web install :	1.3 MB
CC Reporting Web Install:	60 MB
Unified Messaging:	350 MB

Programming Wizards

- There is an intermittent issue which may cause the DECT Configuration wizard to fail. This issue only affects about 250 systems that were shipped out of Nortel Networks as part of the 1st shipment of BCM 2.5's and has been since patched at the factory. If the system version is RC 6.3 version 7.1.8 the patch is already installed. If the version is 7.1.7 the patch may be downloaded from the ITAS web site.
- SR 10399797 - Logging out of a WinNT login session of the BCM will restart the JServ Servlet Engine's running JVM. This results in the deletion of all running, queued, and in-progress wizard instances. This issue will only occur if VNC is active when wizards are being run and someone performs a logout in VNC. The easy workaround for this is to stay out of VNC until the wizards are complete.

BCM Dialup

- There is a known issue with some Operating systems dialing in to the BCM via the BCM's analog modem, which prevents the mapping of network drives from the client to the BCM. The issue exists with Windows 2000 Professional clients, and has been seen on some releases of Windows 95. Windows 98 and Windows NT 4.0 do not have this issue. This affects the following components:
 - BRU (Backup / Restore Utility) normally wants to do it's backups to a drive which is mapped from the client to the BCM. Since a dialup connection is inherently very slowly, we do not normally recommend backing the system up over such a link.
 - Patches use network drives mapped from the client to the BCM.

BRU

- Do not perform Restores to BCM's from different software versions. As well be careful not to restore registries from one system to another unless this is absolutely necessary.
- Netscape is not supported. BRU is an Internet Explorer Application only.
- The BCM should always be rebooted after a restore is done with the BRU.
- An intermittent issue has been seen which when using Windows 95/98 and BRU the BCM seems to need 2 reboots after a restore. Check the system after rebooting once and if the system doesn't seem like it has restored properly reboot the BCM again to workaround this issue.
- The BCM clock shown on BRU is synchronized with the server time only when the page is refreshed.
- The file upload feature only transfers text files. The workaround is to Use FTP or shared folders if file transfer is needed.
- BRU shutdown all voice services when performing a system restore. The services will be restarted as soon as the restore completes. What this means to a customer is DO not perform a restore during business hours.
- The Authentication field under IP Routing->OSPF Global settings always defaults to None after a restore.
- The dial out username/password is not restored, if the user restores the Unified Manager component only. These settings are restored during a full registry restore.
- Time Zone is restored only when the registry is restored. This can affect the voice mail component as it uses the system time as a reference. To ensure proper voice mail operation make sure the time zone and time of the BCM is set before performing a voice applications restore.
- Currently there is an issue with the BRU and the telephony restore. After restoring the telephony the Alarm telephone should read " UTAM key code required" not UTAM Test Failed. The workaround is to enter new UTAM soft key if this occurs. This only affects systems with Companion in the U.S.

Core Telephony

- Seven simultaneous conference calls cause the telephony S/W to perform a reset. This issue was discovered late in the BCM 2.5 testing and existed in BCM 2.0. A patch for this will be available ASAP if needed.
- Currently an issue, which is more prevalent with the T7406 set, whereby the voice path remains open. On the T7406, a key sequence of - pressing IC or Line Key - pressing HOLD key - pressing the Option key is required to get the set into this state. - In this state, the voice path remains open. Once the problem occurs, re-selecting the IC key and pressing the release key will clear the problem.

- Companion Wireless base stations are only supported on the highest DS-30, which can carry a DSM. This would be Module 6 or 7 for a 6-2 DS-30 split and module 6 for a 5-3 DS-30 split.
- SR 30364540 The T7316 sets have too many buttons mapped in Unified Manager. All this issue affects is administrators who program keys need to understand the T7316 doesn't have 34 buttons.
- SR 10437832 The system volume option for telephony sets didn't allow the sets to change the volume on their telephones. Workaround is to change the volume option to use set volume.
- Originating call from DECT through expensive route gives wrong CLID.
- DECT Call Forward No Answer does not work. The work around is for the DECT user to program "Call Forward" on their set.
- DECT has MWI indicator flashing when there is not message for it. This is seen where the deployment is poor. Workaround is to delete the MWI from the set.

IP Telephony

i2004

- SR 10432536 Issue with i2004 and echo on certain types of calls. The echo issue is noticed when people talk over each other or at the same time while on a phone conversation. This issue only occurs when IP set calls to TDM sets, IP sets call to voicemail, and IP Sets call any non-IP trunk.
- SR 10444184 Group listen from the i2004 behaves differently than the normal telephone sets. When group listen is invoked the audio path on the handset of the i2004 is lost and plays from the speaker.
- SR 30363645 IP Clients that are call forward to voice mail and have been disconnected do NOT get voice mail. This impacts remote IP client users as it means the IP client must be active for voice mail to answer. This will be corrected in the Feature Pack of BCM 2.5.
- SR 10431421 i2004 Button programming for F9XX features is not labeled as expected. (Example: F904 should be login but it reads xF904) This will be corrected in the Feature Pack for BCM 2.5.
- SR 10444182 Auto Codec selection for IP clients not working for different Subnets. When a new IP client is installed from a different subnet the BCM is supposed to recognize it is on the different subnet and place the set to G.729. Currently this is not working. The workaround is to set the IP client to the proper codec in Unified Manager. This will be corrected in the Feature Pack for BCM 2.5.
- SR 30365654 An issue where IP client voice quality was affected by the music on hold source. The issue was the MOH source was not the proper specifications.
- SR 10439415 The i2004 can have a call timer active on the set when no call is active. This can happen if the i2004 has a line appearance for a line and

someone from another set is using that line. This feature allows the i2004 to monitor the length of time the line is in use.

- G729 with silence compression on is not supported from the i2004.
- SR 50355982. IP calls got disconnected after 12 hrs on a voice call and then no dial tone on I2004. This is an issue with the I2004 firmware and will be corrected when a fix is available.
- SR 50350812 i2004 does not work with multiple IP addresses. Release Note:I2004 cannot register with BCM when multiple IP addresses are configured on an interface. This happens when the WAN link interface is present and being used as Published IP address. Customers should avoid configuring Multiple IP addresses on an interface at this time when using IP clients.
- SR 50340892 QoS monitoring packets will not go through when NAT is configured on the BCM. The work around is to make the public IP and published IP the same when NAT is configured.
- SR 50347409 I2004 gets stuck in a FW download mode when they try to download the Firmware behind the NAT. The workaround for this issue is to download the firmware from the local BCM or download the firmware without NAT being configured.

I2050

The i2050 requires the BCM DN that it will be using to be configured with handsfree.

- If your using a Xircom modem/ethernet card (esp Dell Notebooks) please insure that you have up-to-date drivers. These PC Cards can cause broken speech issues even when the dock station's NIC is being used.
- For TAPI operation to function properly using the i2050 TSP go to the i2050 Configuration tool then select the PBX tab and select BCM.
- TAPI installation on Windows 2000 and Windows NT requires administrator privileges. This can be achieved temporarily for non-administrators by using the Windows 'install with elevated privileges' feature. If administrator privileges are not used for installation the application will install, but the TSP will not be available. The application will need to be un-installed and then re-installed with administrator privileges to allow TAPI operation.
- For QoS to function properly:
 - Windows 98: RSVP can be enabled - see the QoS tab on the i2050 Configuration tool.
 - Windows 2000: DiffServ, RSVP and 802.1p can be enabled - see the QoS tab on the i2050 Configuration tool. To enable QoS on Windows 2000 the administrator must install QoS Packet Scheduler. This can be done in Windows Network Properties by clicking on "Install...". Then in the "Select Network Component Type" dialogue highlight "Service" and click on "Add...". Then in "Select Network Service" dialogue, highlight "QoS Packet

Scheduler" and click on "OK". The Windows 2000 CD-ROM may be required. RSVP and 802.1p/DiffServ are mutually exclusive. Administrator privileges are required to enable QoS on Win 2000. QoS is a system wide setting, which affects other applications and OS components, the i2050 installation does not assign a value at installation.

- BCM doesn't provide Call Info via UNISTim, therefore the call log features in the i2050 directory do not report results correctly
- Intermittent Mute Issues have been seen on the i2050 client. When this happens the mute will not work on the client. To work around this simply re-mute the i2050.
- An interaction issue with i2050 and Microsoft ISAS (Internet Security and Acceleration Server) has been seen during customer Beta. This happens when the ISAS client is installed on the PC and the firewall option is enabled. When the issue happens the i2050 can crash and even appear to be operating slow. The issue is believed to be a buffering/packet filtering issue with the Microsoft client S/W. The work around for this is to disable the ISAS firewall client.
- A random interaction issue has been seen with the i2050 failing to start after a reboot of the PC. The work around is to simply restart the i2050 S/W.
- If using the Contivity Extranet client on a PC running the i2050 it may be necessary to change the H/W ID in the i2050 configuration. This is necessary if more than one i2050 is connecting using Contivity.

Voice over IP Trunks/Gateway

- The codec renegotiation and, as a result, fax-over-IP calls are currently not supported. This will be looked at for the Feature Pack of BCM 2.5.
- No ring back tone on IP Trunk calls (SR 10437834) and calls disconnected when calling IP trunk from 2.03 to 2.5 through Auto Attendant to i2004 (SR 10441009) This issue has to do with interoperability issues with BCM 2.0X and 2.5. The work around is to upgrade all sites to BCM 2.5.
- SR 104333249 IP trunks do not work with Auto/Disa DN functionality in the BCM. This is normal operation and will be considered in future releases of BCM.
- Long tones are not supported over IP trunks
- For G.729 calls, from an ITG->i2050 there is no speech in the ITG->i2050 direction, regardless of who initiates the call. Work around: Configure the ITG to use G.711 as the preferred codec. A fix for this issue will be in the feature pack for BCM 2.5.
- For proper interoperability with Nortel Networks Meridian 1 ITG, the following configuration guidelines should be adhered to:
 - ITG payload sizes should be set to 30 ms.

- Silence suppression should be configured to the same value on both BCM and ITG (i.e. both on or both off). Silence suppression is called Voice Activity Detection on ITG.
- The profile on the ITG must be set to have the same first preferred codec as the BCM's
- Software on the ITG trunk card should be on 2.X.24 release.
- In order for features such as Transfer and Conference to operate correctly between all BCM's and ITG's in a customer's network, there are some restrictions on the codec preference configuration for IP trunks. In detail, the rules are:
 - The "1st Preferred Codec" for VoIP Trunks must be the same on all BCM's. This is configured in Unified Manager under [Services / IP Telephony / H.323 Trunks / Media Parameters](#).
 - In addition, if the first preferred codec is G.729 or G.723, the Silence Suppression option on that page must be the same on all BCM's.
- M-1/ITG interaction with more than one ITG: when transferring, conferencing, working with 2 or more ITG cards, they must be on the same subnet. If they are not on the same subnet, one-way speech path can be experienced. This problem also occurs with one ITG cards if you program different subnets for each interface. The problem occurs only when a direct media path is set up from an i2004 Internet Telephone on BCM to a Meridian 1 ITG trunk resource on the active Leader card, and the Node IP address is configured (correctly) as a different IP address from the TLAN card IP address. In a single-card ITGT2.x.24 node you can work around the problem by configuring the Node IP address equal to the TLAN card IP address. The Node IP address must be different from the TLAN card IP address if Leader 0 and Leader 1 exist in the node, so the workaround is not always available. A patch for the ITG will be made available as soon as it is available.
- There is an intermittent issue with PEC resources and IP clients where the system will allow calls to try and establish when all resources are busy. This will only happen on extremely busy system and the result is the call will fail. When the DSP resources become available the call can be reattempted.

Voice Applications

Voice Mail

- SR 10445020 An issue exists where the voice mail storage time is limited to 30-40 hours of storage. A problem existed in the BCM S/W that even though there was plenty of hard drive space the voice mail only had 30-40 hours of storage. This issue only affects about 250 systems that were shipped out of Nortel Networks as part of the 1st shipment of BCM 2.5's and has been since patched at the factory. If the system version is RC 6.3 version 7.1.8 the patch is already installed. If the version is 7.1.7 the patch may be downloaded from the ITAS web site.

- A minor issue resulting from the patch and fixed systems above is the message usage report in voice mail will not be accurate. The report will not show all of your available storage time. This will be corrected in the feature pack of BCM 2.5.
- FAX: On external fax calls, voicemail will not recognize a disconnect if the caller hung up during a fax transmission. The line will remain held for the fax transmission for 100 seconds, before the line is freed up.
- An intermittent issue where the Call Pilot Telset Player stops playing messages to a specific DN: Workaround: Dial a different DN, until the BCM can be re-booted.
- In call pilot manager the alternative ext does not detect spaces as illegal name. Workaround is to make sure names are entered properly.
- Unified Messaging Client: Lotus Notes: After a BCM server reboots any lotus notes clients which remained connected to the server during the reboot will appear to have all of the messages disappear from the inbox. To access the messages once again close and restart lotus notes.
- Unified Messaging: When composing a message using the desktop telset player in some cases telset playback will not play the segment of voice previously recorded. Instead the user sees a short piece of silence being played. The workaround is to change the playback device from the telset to the PC speakers and listen via the PC speakers.
- Unified Messaging: Maximum Message Length is not obeyed: Users can send messages longer than the defined COS limit.
- Unified Messaging: Outlook Express 5.0 does not update message read status correctly: Message read status does not change. Workaround: Upgrade to Outlook Express 5.5 or 6.0.
- Eudora Unified Messaging does not indicate mailbox locked status.
- In some cases Windows 2000 installations will not be able to send fax attachments using outlook express. This issue will be corrected in a patch as soon as possible.
- Intermittent Unified Messaging NMDCFM32 Error when sending multiple files. Workaround: Attempt to attach the files and send again.
- Unified Messaging issue: Digital Networking Addressing Incorrect: User cannot "reply" or "forward" messages that have been received via VPIM or AMIS. Workaround: Use the telephone set to reply or forward these types of messages.
- In certain cases a mailbox number or site prefix will also correspond to a command in some context. Workaround: In a context where a clash occurs use a different prefix/number.
- In a fax on demand mailbox the login Soft Key does not work from F980. Workaround is to use feature 981.

- Australian voice prompts have some cut-off prompts. Also some actions concerning operator revert, special addressing, do not match the voice prompts in this release. This only affects the Australian prompts.

Call Center & Call Center Reporting

- it is possible to enable the MIS reporting keycode before Informal Call Center or Professional Call Center is enabled. If MIS reporting is applied first the Professional Call Center stand alone keycode can not be entered successfully. In this situation after the application and rejection of the Professional Call Center keycode the Professional Call Center functionality is available even though the Professional Call Center keycode is not in the installed options list. Workaround: Ensure that the Informal Call Center or Professional all Center keycode is applied before the MIS reporting keycode is enabled. This will be fixed in the Feature Pack for BCM 2.5.
- Headset for Supervisor monitor doesn't work as expected with Business Series sets: Workaround: Hit the mute/un-mute button on the set.
- SR 10439869 Call Center Reporting: After an extended period of time the status on the real time screen gets out of sync with each other. When this happens one screen can show different info than the next. Workaround: Restart the RDB server.
- SR 10431466 Call Center Reporting: Companion sets with Answer DN's that answer call center calls do NOT report properly in the reporting and status screens.
- Call Center Reporting: Summary Report Graphs are not displaying: Retry graphical view button and then summary button until it displays correctly.
- Call Center Reporting: Overflow calls not logged correctly: Workaround is to have agents only logged into a single skillset instead of multiple ones. If this is not possible, ignore the specific skillsets overflowed to in the "Incoming Call Report Lines" Report.
- Call Center Reporting: Large negative numbers are being displayed in some reports; these values are bogus and should be ignored.
- Call Center Reporting: Cannot remove wallboard messages: Workaround is not to remove message but to edit text of message.
- Call Center Reporting: GUI Inconsistencies in Call Center Reporting: When looking at reports there is no clear way to get back to the status/main screen. To do this you have to close the window.
- An intermittent issue has been seen where a second mailbox can be created for a skillset. This only happens when the control DN for the skillset is changed multiple times in succession. Workaround is to refrain from changing skillset CDN a lot.
- Skillset mode did not change from day when night routing was added. Workaround is for user to use F982 to change this setting.

- An issue with Caller Input Rules. # after max digits is not seen as a termination key. Workaround is to use fixed digit lengths.
- Supervisor disconnected from the call when an agent is forced off. Workaround is to not force off Agents when a supervisor is on call.
- An intermittent issue has been seen where the Call Center Reporting shows agent on incoming call when the agent is available. Workaround is to logout and log back in to clear problem.
- An incorrect display for a Wallboard is shown after a disconnect while agent's set is ringing. Workaround is to reset the wallboard.

Voice Button

- Voice Button calls are terminated only when both the PSTN and IP sides are closed – this can lead to an agent getting two live calls at the same time. Workaround end the IP Session and voice session when the call is finished and make sure the break time is sufficient to allow for this to happen.
- Voice button does not work with Auto-Answer for agents.
- Voice button does not support frames on web pages in which the application will be navigated to. Workaround is to not use or navigate to web pages with frames.
- SR 30365377 The voice button client will only work if the Java Run Time S/W is installed on the client PC. This can be found at <http://javasoft.com>
- SR 30364822 Intermittent Voice Button Client will not install from Web Page. Workaround is to use NortelDT shared folder to install the client.
- SR 30364844 When using Voice Button callers Telset is answered and the CC agents set rings 7secs later. Workaround: Ensure dialing plan is correct with respect to public DN lengths. This will ensure quicker dialing.
- When Call Center tries to call a customer if that number is wrong, then it is possible that a PRI trunk will be used and then it waits for more information to dial out or it gives fast busy. ACD will reroute this call to an agent anyway. Workaround: Make sure dialing plan is correct so wrong numbers are avoided.
- Issue with Voice Button & Call Center reporting when a call is cleared down. Workaround is to End browser session before ending voice call.

LAN CTE

- An issue with LAN CTE where applications cannot control (drop/hold/transfer) a priority call. As well applications cannot control a set which is in a manual session initiated by the user. This includes any feature requiring further user input (eg. transfers, set forwarding, paging, park).
- A problem has been seen with LAN CTE clients stop functioning due to the LAN CTE server component going down. This problem has only been

seen to occur when the connection to the BCM system is established and then broken numerous times in succession and then an error occurs.

Workaround: Ensure the network is clean between the BCM and client.

- LAN CTE and TAPI clients will not operate through NAT.
- An issue has been seen in Windows 2000 with the Active Directory providing the network names, the NetBIOS name appears to be the fully qualified domain name, example "pc1.nortel.com". The actual NetBIOS name is "pc1" and this is the value that should be entered into the Machine Name identifier section of the LAN CTE Configuration table. Another way of looking at it is that the NetBIOS name will not contain the character "." so if it appears to, use all of the characters before the period as the machine name identifier.
- An intermittent issue has been seen uninstalling LAN CTE. If this occurs simply re-install and then uninstall the application.

Call Detail Recording (CDR)

- There is no error handling in administration of the account code Feature code. If the Account Code Feature code is in use by another application, no error will be reported.

Personal Call Manager (PCM)

- No known issues.

Attendant Console

- SR 10439873 An issue has been seen where the Attendant Console can lose the status of calls. This occurs when an intercom call gets put on hold on the console and then that intercom caller places the call on hold. If the console then answers another call the on hold call is lost. Workaround: The call is still on the telephone set and can be answered.
- SR 30365378 An issue in German and Danish markets with the Attendant Console showing Callback(in orange) instead of calling. Workaround: remove the period in the line names for the BCM. The period in Itg. Causes the PC based attendant console to misbehave and needs to be removed from the default line name.
- Entering a key code for Attendant Console Seats produces the error dialog stating "Component could not be contacted". The Console Service is not automatically started by default on BCM 2.5 and it must be started to be able to process the Attendant Console Seats key code. The service can take 30 minutes to start the 1st time it is started.
- If when starting up the Attendant Console Client, connectivity is lost and regained repeatedly in a short period of time, the client may be a different version than the Attendant Console Server on the Business Communications Manager system. The client and server must be at the same version in order to properly obtain a connection. The version

number of the client can be found in the About section of the Help drop down menu. This issue may occur if someone has a BCM 2.0 version of client and tries to connect to 2.5.

Data Components

General

- When changing the IP address of a NIC, not all of the related settings will be changed as well. It is therefore important to make alterations in any of the following areas that are being used:
 - Check the DHCP setting for the NIC whose IP you changed. “Scope Status” will be reset to “enabled” and must be changed to “disabled” if that is what you want.
 - The Global Options for the “Nortel IP Terminal Information” will not be reset. If the published IP address is for the NIC with the changed IP address, then manually change the IP address in this field.
 - NAT does not reset the IP address in the rules. Disable then re-enable default rules for the interface that’s IP has changed.
- There is a maximum of 16 ISDN B-channels that can be used for ISDN Dialup. BCM supports 32 Demand dial interfaces to add, configure and use. Having 32 interfaces may cause loading time of Unified manager to increase and user may run in to problems logging in to Unified Manager. This limitation comes from the DCOM time-out to load the Unified manager. It is recommended to add only the needed number of interfaces. The recommended maximum number of interfaces is 16, to make BCM work optimally.
- An issue with ISDN Dialup where the BCM receiving a request to connect does not restrict access to channels. If only one channel is configured on the BCM receiving the request to connect, all requests, up to 16 channels, will be granted.
- If RIP is applied on the ISDN PRI Interface, Routing Table Update must be changed from On Demand to Periodic, or Routing Table will not advertise routes for PRI Interface
- Fast Path routing from LAN to LAN interface is not supported with QoS, Firewall filters, NAT or IPSec. Workaround: Disable Fast path routing.
- Although the BCM is capable of providing optimal bandwidth allocation, it is often seen that at least 40% of traffic load of the total LAN bandwidth MAY corrupt LAN-to-LAN packet forwarding. The default setting of a traffic-smoothing rate at 40Mbps causes this. To overcome this throughput limitation, the user can choose either to change the rate from default or to disable the traffic smoothing. The following should be considered during network deployment:
- If QoS is used for LAN, customer SHOULD not use more than 10%-to-20% traffic load of 100Mbps for LAN-to-LAN forwarding in case of using a small packet size such as 64bytes.

- For general transmission using fast forwarding, customer SHOULD not apply more than 35% of traffic load considering 100Mbps traffic bandwidth for the LAN in case of a small packet size such as 64bytes. If this is exceeded the BCM can become unstable. The workaround is to set a reasonable traffic-smoothing rate based on active data applications.

IP Routing

- Although BCM supports various routing protocols, customer MUST observe the following restrictions before and after routing implementation:
- SR 50350601 OSPF should not be used when Multiple IP addresses are configured on an interface. OSPF will not announce the routes correctly.. Workaround: Avoid using OSPF when multiple IP addresses are configured on an interface.
- SR# 50319822 Rip announces all networks on local interfaces even if the interfaces are disabled.
- The BCM must be rebooted before configuring routing on it if the IP address of the interfaces is changed.
- The router priority in OSPF for BCM cannot be set to zero so that it becomes router other than DR (Designated Router) or BDR (Backup Designated Router). Workaround: Set the BCM router priority to lowest and also set the router priority of the backbone/core router to a higher value so that the BCM does not become DR or BDR.

IPX Routing

- IPX Routing is not installed by default any longer in BCM 2.5. Customers that need this functionality will need to install IPX from the maintenance area of Unified Manager.
- SR 50317760 IPXPING is not supported.
- Intermittent install issue with IPX. If IPX does not get installed in first attempt, user should try a second attempt. In certain cases, users will need to run IPX install twice from the wizard.
- V.90 Modem backup interface is not supported with IPX.
- For IPX WAN connection via Frame Relay, user must choose default frame size as 1500. The frame size must not be altered.
- Enable SAP before entering IPX static services.
- When IPX static routes are configured, IPX clients (Microsoft client for Win98/NT) may required to reboot to find all available servers on the LAN/WAN.
- The user is not required to assign net number/frame type to the BCM 's interface when IPX server exists on that particular interface(s). The server will assign net number to BCM 's interface accordingly.

Policy COPS Static/Dynamic

- In Services |Policy Management | QoS |Rules, add an IP Filter Group Entry with more than 31 IP filters will cause the error message "Not enough memory. Interface Manager Out of memory" to show up and eventually cause the miserver to hang. Reason: The maximum IP filters allowed per IP filter group are 31. But the object manager does not reject the user input for more than 31 IP filters in an IP filter group in the current release. Workaround: Put only up to 31 IP filters in an IP filter group. To recover: Remove the file named "ipFGrp.qpa" from directory "C:\program files\Nortel Networks\Policy Services\Config". Note that this will cause all the entries in the IP Filter Group to be gone.
- SR 60335290 Dynamic policies will get partially downloaded to BCM unless a refresh is done. After enabling the dynamic management mode the unified manager need to refresh a couple of times to get the entire policies downloaded to the BCM from OPS (Optivity Policy Server) as it may be still in the process of downloading the policies. The workaround is to refresh the Policy Management a couple of times to get the entire policies downloaded.
- SR 50350305 When the user creates multiple Policy server IP addresses it takes longer for the BCM to go from Static mode to Dynamic Mode. This issue occurs because the Policy Server needs some time to download policies from the server. The time really depends on the number of retry times..
- OSPFIGP traffic condition is not supported by BCM. BCM treats OSPFIGP traffic as Premium traffic by default.
- Policies are not displayed in order of the order number in Unified Manager. This will be fixed in the feature pack of BCM 2.5.
- SR 50355179 QoS drop rule is not enforced immediately after rebooting BCM. The drop rule is not enforced for about 12 seconds after rebooting the BCM.
- Longevity for Expire Immediately may actually take 2-3 minutes to take affect. This will be fixed in the feature pack of BCM 2.5.
- SR 60335159 Right now it is not possible to check the status of the OPS Server from the Unified Manager. Work around - After enabling the dynamic management, the policy management status will come to the disabled state if it can't get connected to the OPS so that user can know that BCM is still not connected to OPS.
- Refresh is required in Unified Manager after the dynamic management status has changed from disabled to enabled.

DHCP

- Some times the clients on remote network cannot get the IP address from DHCP Server. Solution: This is due to the fact that LAN interfaces getting added to the DHCP Relay agent on DHCP Server after Reboot. This

problem happens whenever the BCM is rebooted. Workaround: Disable the DHCP Server and Enable it to resolve the problem.

- When the address range is modified, exclude address range disappears. Solution: This behavior is by design intent. Exclude address is deleted from the database when the address range is modified.
- When the IP address/subnet mask of LAN1 or LAN2 is changed DHCP LAN1 and LAN2 configuration disappears. Solution: Changing the IP address/subnet mask of BCM LAN interfaces will trigger the DHCP Scope to be reinitialized. That means user will lose the original address range, exclude list, reserved address list and scope options.
- An IP address cannot be put under an exclude address range. Solution: Once the IP address has been leased by the DHCP Server, it will be in the DHCP database for the selected lease period. During this time user cannot put this address in the Exclude list even if the client has released the address. Workaround: Wait until lease end.
- Lease information is not displayed in Unified Manager. This will be corrected in the Feature Pack of BCM 2.5.

QoS

- PPTP tunnels and IPSec tunnels with the same endpoints are not supported.
- NAT, Firewall, and QoS through PPTP tunnels is not supported.
- With LAN Fast Routing enabled, NAT, Firewall, QoS, and IPSec are not supported on those interfaces..
- QoS on the I2004 does not work with multiple IP addresses.

IPSec

- IPSec and PPTP tunnels with the same endpoints are not supported.
- IPSec is limited to 20 tunnels per system and 16 Local and 16 Remote Accessible Networks per tunnel.
- In order to route packets through the tunnel a static route to the other side of the tunnel must be configured.
- Should there be a problem of any sort, to determine if the tunnel is up, check the Event Log. The Event Log will also contain error messages if the tunnel has not come up. Depending on the problem, you may not see any error messages if the log you are looking at is on the remote side of the tunnel.
- Perfect Forward Secrecy(PFS) behaves as follows:
 - If the responder has PFS Enabled and the initiator has PFS Disabled, then an IPSec tunnel will NOT be set up.
 - If the responder has PFS Disabled and the initiator has PFS Enabled, then an IPSec tunnel (not using PFS) will be set up.

- When connecting a BCM to a Contivity Extranet Switch (CES): On the CES, you must turn off Vendor ID and Compression. We also do not support RIP with the CES. If you are going to use NAT on the BCM side, the BCM and the CES cannot be on the same subnet. The CES will not allow the BCM IP address as a Remote Accessible gateway.
- SR 50346279 BCM 2.5 IPsec RIP Protocol is not compatible between BCM 2.5 and CES Contivity Extranet Switch.
- SR 50355983 QoS filter order number does not take effect on the rules for IPSEC
- SR60348348 If the local access number is deleted the network number will be renamed.
- SR 50356910 Issue with IPsec and ISDN Dialup as follows: Configure 2 BCM's as follows: 1 ISDN connection to an ISP with NAT enabled, 1 ISDN connection to the other BCM with no NAT. Both ISDN interfaces have IPsec tunnels configured. The IPsec tunnel through the ISP is connected to the 2nd BCM ISDN interface. Both tunnels are enabled and the global status is enabled. Start pings over both interfaces. Now, disable the 1st tunnel locally on both BCM's. You will see the pings come back as the tunnel is completely disabled. Now if you disable the 2nd tunnel locally on only one side, the pings will still continue, which should not be the case. The packets over the 2nd tunnel should have dropped.
- SR 50356708 Issue with IPsec when BCM to BCM with IPsec tunnel and Enable Networks Address Translation "NAT" and user can not FTP from BCM 1 client PC to BCM 2 client NT server.

PPTP

- When configuring PPTP do not create a static route to the other side of the tunnel. Packets will not be sent through the tunnel if you do. PPTP will setup the necessary routes when the tunnel is enabled.
- PPTP and IPsec tunnel with the same endpoints are not supported.
- SR -60343747 The PPTP Tunnel gets connected even after deleting the tunnel on the remote end. Suppose we have a PPTP Tunnel and if we delete the tunnel on the remote side and try to connect from the local side it still gets connected. Workaround - While deleting the tunnel, also delete the username from User Manager in Unified Manager. The username is same as tunnel name.
- If a PPTP Tunnel is created across two BCM's (Branch to Branch) the link over the tunnel will not get established if the static IP Address pool on both BCM are on the same subnet. By default the static IP Address pool is 10.10.14.0. Workaround - Configure two BCM's in different static IP address pool. To change it go to Resources->Dialup page of Unified manager.
- SR 50352661 Networks Address Translation (NAT) is not compatible and is not supported in BCM2.5 with PPTP.

- SR 50343910 Under TUNNEL LINK PARAMETERS when the Connection Type is set to “Persistent” user should not enter any value under Idle timeout, if user select the Connection type to “Persistent” and also enter the value on the Idle timeout it will create a conflict. This is because “Persistent” means connecting all the time and Idle time out is for “ On demand”.
- SR 50348012 “Destination Networks” will not detect duplicate DESTINATION NETWORK ADDRESS entry. For Example: If the user adds the DESTINATION NETWORK ADDRESS of 10.10.10.0 and subnet mask of 255.255.255.0 it will show up in Unified Manager. Now if the user tries to add the same destination network address again, Unified Manager will not give error message. Workaround – ensure the PPTP tunnels are configured properly.
- SR 50344845 If the PPTP tunnel is already up between BCM to BCM and a user tries to disable the PPTP interface by changing the status from “Up” to “Disable” this will not disable the PPTP interface at all, the data traffic will still go through the tunnel. The proper step to disable the PPTP tunnel is changing status from “Up” TO “Down” and “Disable”.
- SR 50349262 Remote dialing from Win NT workstation: When user creates a PPTP VPN tunnel from Win NT workstation from Home Office to a BCM. After the tunnel has been established, home office can access the clients behind the BCM. However clients behind the BCM cannot access the Home office. For ex, A Win NT workstation (10.10.10.100) from home office remotely connected (PPTP) to BCM LAN1 (10.10.10.1), A client (10.10.11.100) on BCM LAN2 (10.10.11.1) cannot ping or send any traffic to remote Win NT workstation (10.10.10.100). However Win NT workstation (10.10.10.100) can send the traffic to client behind the BCM (10.10.11.100).
- SR 50352659 PPTP is not supported on an ISDN or V.90 Modem connection form the BCM.

Firewall

- The Firewall is limited to 32 inbound and 32 outbound rules per interface.
- Logging: Be aware that if you setup your Firewall Filters to log ALL traffic, the logs files will get VERY large. If you wish to view the logs, the process will take a very long time to display and the Unified Manager will not be usable until the log has been brought up on the viewer. To work around this limitation, setup your logs to only log errors (setting 1). This will reduce the amount of logged traffic.
- Disabling Firewall In Case of Emergency: As with any firewall, it is possible to mis-configure the BCM's firewall in such a way so as to completely lock yourself out of the system, creating a situation where it is impossible to get in to fix the problem. In such a circumstance one must log into the BCM's command-line console and issue the 'fltdisable'

command. When you access Unified Manager, you will need to go to the Firewall Filter section and set the status to Disable. This utility does not update the registry, but by setting the status, the registry will be updated. Then the firewall rules can be fixed before enabling them again.

- **Dynamic IP Type:** For both Source and Destination: Dynamic refers to IP addresses that are remote assigned, i.e. your ISP assigns your IP address via DHCP or similar. This does not mean to match to any IP address. Use 0.0.0.0 with a mask of 0.0.0.0 to match to all IP addresses.
- **Default Rules:** The choice of 'Disabled - Pass all' means that no Firewall checking will occur on this interface. Setting an Incoming Rule that will block all incoming and Default Rules is set to disabled, is not the equivalent of setting the Default Rules to Enabled (either with or without IP phones). In the first case, packets that originate from inside the firewall are not treated as stateful. When a response packet is returned, it will match the Incoming Rule and will be blocked. In the second case, the outgoing packet will be treated as stateful, so when the response packet will match the existing state and will be allowed back in.
- If access to Unified Manager is desired through the Firewall you will need to set up 3 Input Rules, one for RPC, one for DCOM, and one for port 6800. They should each look like the following:

Direction	In
Protocol	TCP/UDP
Destination IP Type	Fixed (or Dynamic, if remote assigned)
Destination IP	IP address of this interface (or blank if remote assigned)
Destination IP Mask	Appropriate mask (or blank if remote assigned)
Destination Port Range	RPC (2nd Rule: DCOM, 3rd Rule: 6800)
Source IP Type	Fixed
Source IP	IP address of the system that will access BCM
Source IP Mask	255.255.255.225 (or as appropriate)
Source Port Range	All

|

Rule Order does not matter, as long as these rules come before more general rules.

- **IP Options and Source Routing:** Setting these to Allow means that this rule will match ONLY if the IP packet has IP options/source routing option set. Setting it to Deny means that it will match ONLY on packets that do not have these fields set. Setting it to Ignore means that these fields will not be checked and therefore all packets will match.
- **Firewall Filters with i2004 phones:** In Firewall Filters when you set 'Enabled - Pass outgoing and Block incoming except IP phones' this only allows an IP phone to register with the BCM through the firewall. You still must set up an H.323 rule to allow the voice traffic through. For example, set Default Rules to 'Enabled - Pass outgoing and Block incoming except IP phones' and set an incoming H.323 rule like:

Stateful:	Yes
Disposition:	Pass
Protocol:	TCP/UDP

Source IP: <IP address or subnet of IP phone outside firewall>
Source Port Range : ALL
Destination IP: <appropriate inbound IP address/subnet>
Destination Port Range: H.323

- Firewall Filters & IPSec configuration: To use the default rules with IPSec, you need to include firewall rules that will allow IPSec packets in. The default rules will work on packets going through the tunnel. So, add the following Input Filter Rules:

Stateful: Yes
Disposition: Pass
Protocol: IPSEC_ESP
Source IP: <Remote Endpoint Address>
Source Range Mask: 255.255.255.255
Destination IP: <Local Endpoint address>
Destination Range Mask: 255.255.255.255

Stateful: Yes
Disposition: Pass
Protocol: IPSEC_AH
Source IP: <Remote Endpoint Address>
Source Range Mask: 255.255.255.255
Destination IP: <Local Endpoint address>
Destination Range Mask: 255.255.255.255

Stateful: Yes
Disposition: Pass
Protocol: UDP
Source IP: <Remote Endpoint Address>
Source Range Mask: 255.255.255.255
Source Port Range: 500
Destination IP: <Local Endpoint address>
Destination Range Mask: 255.255.255.255
Destination Port Range : 500

- An issue exists with the following configuration: 2 BCM's are setup to have their Net Link Manager Next Hops set to each other and Firewall Filters are enabled with Default Rules enabled.

Net Link Manager will have a problem with this as the Firewall is blocking its packets from reaching the other BCM. This will cause strange behavior with the Firewall and the connection. To get around this security mechanism, you should configure an inbound rule on each BCM that will allow ICMP packets in originating from the other BCM and terminating at itself. i.e. if you have BCM's with the following IP addresses: 10.10.10.2 & 10.10.10.4

On BCM with IP 10.10.10.2

Stateful: Yes
Disposition: Pass
Protocol: ICMP

Source IP: 10.10.10.4
Source Range Mask: 255.255.255.255
Destination IP: 10.10.10.2
Destination Range Mask: 255.255.255.255

- Firewall must be disabled and re-enabled after making any additions or changes to filters or rules.
- If Firewall is enabled and a routing protocol is used, you should implement rules to allow Routing protocol to pass.

Network Address Translation

- Currently BCM does NOT support IP clients through its NAT implementation. This issue only affects about 250 systems that were shipped out of Nortel Networks as part of the 1st shipment of BCM 2.5's and has been since patched at the factory. If the system version is RC 6.3 version 7.1.8 the patch is already installed. If the version is 7.1.7 the patch may be downloaded from the ITAS web site.
- NAT is limited to 32 rules per interface.
- An issue in NAT currently will only allow support of one FTP server behind the BCM when using NAT. This one server must be mapped to the FTP port on the private side of the BCM.
- Dynamic IP Type: For both Private and Public: Dynamic refers to IP addresses that are remote assigned, i.e. your ISP assigns your IP address via DHCP or similar. This does not mean to match to any IP address. Use 0.0.0.0 with a mask of 0.0.0.0 to match to all IP addresses.
- BCM behind a BCM acting as a router using NAT: You cannot manage a BCM through another BCM when it is on the private side of a NAT'd interface.
- NAT must be disabled and re-enabled after making any additions or changes to filters or rules.
- If you configure a Backup Dial-up Interface, you should implement rules to allow Net Link Manager to send ICMP and receive reply from Next Hop on Primary Link address.
- If you are using a Frame Relay WAN link to connect through a BCM for NAT purposes, you must set your frame size for the WAN link to 1524.

WAN using Frame Relay & PPP

- SR# 60321832 An issue exists between BayRS routers and BCM if the when compression is enabled. This is a compatibility issue with BayRS routers. It is recommended not using compression if the remote router is a BayRS router.
- When using PPP compression between BCM's keep the frame size set to 1600.
- The Frame size on the WAN interface must be set to 1524 for Internet Browsing over WAN link.

- When the PPP link is up and authentication is enabled, disconnection of the link cable and connecting it back for several times may cause the BCM to crash. Avoid excessive removal of the WAN cable while it is being used.
- When using the BCM as a frame relay DCE device and having it disconnected for 20+ minutes, BCM may crash. It happens when both WAN interfaces on BCM are configured and connected to other BCM/FR device, and either one or both interfaces are disconnected for 20+ minutes. In the special case where BCM is used as DCE and two WAN interfaces have been configured, the workaround is not to disconnect the WAN link physically for an extended period of time.